AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

I, Michael Agostinho, being duly sworn, depose and state as follows:

INTRODUCTION

1. I am a Special Agent with United States Department of Homeland Security (DHS), Immigrations and Customs Enforcement (ICE), Homeland Security Investigations (HSI), and am assigned to the office of the Resident Agent in Charge, Providence, RI. I have been an agent of HSI since 2008. As part of my duties, I am authorized to investigate violations of the laws of the United States, including criminal violations relating to child exploitation, child pornography, coercion and enticement, and transportation of minors, including but not limited to, violations of 18 U.S.C. §§ 1470, 2252, and 2422. I have received training in the investigation of child pornography, child exploitation, and transportation of minors, and have had the opportunity to observe and review examples of child pornography (as defined in 18 U.S.C. § 2256).
2. I am currently participating in an investigation relating to violations of federal law by Richard SENECAL for attempted coercion and enticement of a minor in violation of 18 U.S.C. §§ 2422(b). I submit this affidavit in support of an application to search the content of a black Motorola Schok cell phone ("TARGET DEVICE ") or media located therein, as more fully described in Attachment A, which is incorporated herein by reference; and to seize evidence, instrumentalities, fruits of crime, and contraband as more fully described in Attachment B, which is also incorporated herein by reference.
3. The statements in this affidavit are based in part on information provided by Forensic Analysts (FA) of the Rhode Island State Police ("RISP") Internet Crimes Against Children ("ICAC") Task Force, other HSI agents, and Detectives of the RISP ICAC.

BACKGROUND OF THE INVESTIGATION AND PROBABLE CAUSE

4. During the month of October 2021, Detective Adam Houston, of the RISP ICAC, was conducting an online child exploitation investigation on Grindr, a geo-social networking mobile application geared towards gay and bisexual men. On October 5, 2021, Detective Houston was working in an undercover capacity, portraying himself as a fourteen (14) year-old male on the aforementioned mobile application. While acting in an undercover capacity, Detective Houston received a message from a person utilizing the Grindr username, "Rickbbpig" stating, "Hi what's up." Detective Houston viewed the profile associated with the account which identified "Rickbbpig" as sixty-one (61) years-old. Furthermore, the user wrote "*looking for other pigs"* in the "About me" section of his profile. In addition, there was an image attached to the profile which depicted an adult white male with a beard. The user further described himself as:

> **Height:** 6'1'
> **Weight:** 220 lb
> **Ethnicity:** White
> **Body Type:** Average
> **Gender:** Man
> **Pronouns:** He/Him?his
> **Position:** Versatile
> **Tribes:** Bear, Daddy, Poz
> **Relationship Status:** Single
> **Looking For:** Dates, Right Now
> **HIV Status:** Positive, Undetectable
> **Last Tested:** October 2020
> **Meet At:** Your Place
> **Accepts NSFW Pics:** Yes Please

5. On October 5, 2021, Det. Houston responded to the user in an undercover capacity and the following conversation ensued:

> **Undercover: What's up**
> *Rickbbpig: Horny u*

Undercover: Always
Rickbbpig: Into
Undercover: Text me 4014094589

6. The conversation then continued through text messages where Det. Houston identified himself as a fourteen (14) year-old boy. The suspect utilized telephone number, (727)244-9274.

7. The conversation is transcribed below:

2021/10/05	02:29:06 PM EDT	727-244-9274	SMS	Incoming	Hi rickbbpig here
2021/10/05	02:29:26 PM EDT	727-244-9274	SMS	Outgoing	hey!!
2021/10/05	02:31:23 PM EDT	727-244-9274	SMS	Incoming	Into open versatile u
2021/10/05	02:31:37 PM EDT	727-244-9274	SMS	Outgoing	same
2021/10/05	02:31:45 PM EDT	727-244-9274	SMS	Outgoing	i cant host tho
2021/10/05	02:31:50 PM EDT	727-244-9274	SMS	Outgoing	i dont drive either...im only 14
2021/10/05	02:31:55 PM EDT	727-244-9274	SMS	Incoming	Me either
2021/10/05	02:32:13 PM EDT	727-244-9274	SMS	Incoming	Really?
2021/10/05	02:32:13 PM EDT	727-244-9274	SMS	Outgoing	well that makes it harder lol
2021/10/05	02:32:33 PM EDT	727-244-9274	SMS	Outgoing	yea 😈
2021/10/05	02:32:47 PM EDT	727-244-9274	SMS	Incoming	But you have no problem having sex with men
2021/10/05	02:33:06 PM EDT	727-244-9274	SMS	Outgoing	nope
2021/10/05	02:33:18	727-244-9274	SMS	Incoming	Cool

8. Over the course of the next two days, the user disseminated the following images to Detective Houston, whom he believed to be a 14 year old boy:

a. nude image of an adult male's penis

b. nude image of an adult male's anus

c. Nude image of an adult male's erect penis

9. Additionally, also on October 5, 2021, the suspect solicited the undercover agent, a person he believed to be a 14-year-old boy for sexual intercourse on communicated with the 14-year-old boy about narcotics to include methamphetamine and marijuana. After numerous texts spanning October 5 and October 6, 2021, the suspect and the undercover officer agreed to meet at a location in Warwick, RI, with a plan to return the purported 14 year old's nearby residence to have sexual intercourse.

10. The suspect was subsequently identified as Richard SENECAL (1960), after he arrived to have sexual intercourse with a 14-year-old boy. SENECAL was arrested by the Rhode Island State Police and issued his Miranda rights. SENECAL waived his rights and made the following statements, among others:

- SENECAL stated he was aware that the person he was talking to was 14-years old
- SENECAL also stated that sending nude images and requesting nude images of a 14-year-old was against the law.
- SENECAL admitted that he planned on having sexual intercourse with the 14-year-old boy during the fictitious meeting.

11. SENECAL was charged in Kent County Superior Court with three (3) counts of Electronically Disseminating Indecent Material to a Minor and two (2) counts of Indecent Solicitation of a Child (Case # K2-2022-0041A). SENECAL was subsequently released on $1,000 surety bail.

12. During the month of April 2022, Detective Corporal Luke Schatz, a member of the Rhode Island State Police (RISP) Internet Crimes Against Children (ICAC) Task Force, was conducting an online child exploitation investigation on *www.nastykinkpigs.com*, a social networking site, similar to Facebook, but for the gay fetish and kinky community. A user can post advertisements, join groups, request friends, and chat with other users. Users can send messages directly to other users or they can send a user an "Oink". An "Oink" is sent from one user to another to alert that user that the sending user is interested in them. When an individual joins Nastykinkpigs.com, they must create a profile. Nastykinkpigs.com requires users to be eighteen (18) years of age. They require users to enter a date of birth, showing they are at least 18, but they do not verify this date of birth. Based on my training and experience, I know that juveniles will create accounts on sites such as Nastykinkpigs and portray themselves as being 18 years of age or older. I also know that individuals looking to identify and exploit juveniles may use sites, such as Nastykinkpigs to solicit these juveniles.

13. On April 4, 2022, Detective Corporal Schatz was working in an undercover capacity, using a profile on Nastykinkpigs.com. Detective Corporal Schatz received an "Oink" from a profile identified as *Richards*. This profile had four (4) images associated with it. Two (2) images were photographs of a white male's face. The remaining two (2) images depicted an adult male penis and an adult male spreading his buttocks and exposing his anus. The profile listed the account holder as a 62-year-old male from Warwick, Rhode Island. After viewing the images in the *Richards* profile, Detective Corporal Schatz immediately recognized the white male as Richard SENECAL, the individual the RISP ICAC Task Force arrested on October 6, 2021 for Indecent Solicitation of a Child and

Electronically Disseminating Indecent Material to a Minor. SENECAL was presently released on bail for those charges.

14. On April 5, 2022, Detective Corporal Schatz responded to SENECAL's "Oink" with the following message, "Hey I'm from Warwick too!" The following conversation on Nastykinkpigs.com ensued. The chat communications described below are quoted verbatim including any misspellings and grammatical errors:

Senecal:	**U host and slam**
Undercover:	yea r u cool if im younger…want to text instead?
Undercover:	I prob could…u cool if im younger…it would be easier to text I think if that works
Senecal:	**yes as long as you are pig [pig emoji inserted] and kinky here's my number 978-754-5889 rick**
Senecal:	**[Sends an "Oink"]**
Senecal:	**Sent you my number to we can text yes fine that you are younger here it is again 978-754-5889 rick**

15. On April 5, Detective Corporal Schatz contacted SENECAL using an undercover state police telephone number and sent the following text message, "Hey! Dylan from NKP". Detective Corporal Schatz and SENECAL engaged in a conversation via text message where Detective Corporal Schatz identified himself as a 14-year-old male. After identifying himself as a 14-year-old male, SENECAL indecently solicited him, an individual who he believed was a 14-year-old male, to engage in sexual contact and send nude images. SENECAL also solicited to use the illegal stimulant methamphetamine with him and sent an image of his penis and anus. The following is an excerpt from the text message conversation between Detective Corporal Schatz and SENECAL:

Senecal:	**What's up**
Senecal:	**Rick here**

Undercover:	Hey nothing much, thanks for texting, it's hard for me to use that site at school! Lolol
Senecal:	**What do you want get into**
Senecal:	**Tollgate**
Undercover:	Yea a freshman…school sucks btw Lolol
Senecal:	**Or college**
Senecal:	**Graduated in 1979**
Undercover:	Nah high school…wish I was older, it's hard to find people my age that are same know what I mean
Undercover:	Wow!
Undercover:	Did u go to Tollgate too?!
Senecal:	**Yes took computer technology**
Undercover:	Cool! Well I'm 14, def into computers…can't wait for 2 more years when I can drive!
Undercover:	I'm glad you're cool with that!
Senecal:	**Ok so what do you wanna get into**
Undercover:	I mean I odn't have a lot of experience…I'm def curious about everything. What do you think? Btw I like ur mustache in your NKP pics
Senecal:	**Thanks**
Senecal:	**Open and love to party**
Undercover:	Oh cool, so what would u want to do?
Senecal:	**Everything**
Undercover:	[One (1) winking and one (1) smiling emoji inserted]
Senecal:	**U use a syringe**
Undercover:	For Tina? Only used it once and smoked it…it's hard o find stuff at my age…but my mom is always at her bfs so I'm pretty much home alone a lot
Senecal:	**To inject T**[1]
Undercover:	Guess I've grown up fast, not sure if that makes me a loser or not
Senecal:	**No**
Undercover:	[smiling emoji inserted]
Senecal:	**I work**
Senecal:	**Sorry do you work I'm retired**
Undercover:	Do I work?
Senecal:	**yes I did at 14 with working papers**
Undercover:	Really?! No I with I did to make some money
Undercover:	Do you have T?
Senecal:	**I can get**
Undercover:	I liked the way it made me feel when I did it
Senecal:	**And we are pointing**
Undercover:	What?

[1] I know from training and experience that "Tina" and "T" refer to the illegal stimulant methamphetamine.

Senecal:	**Horny as fuck**
Undercover:	Omg me too
Senecal:	**Using a syringe to inject it into you and me**
Undercover:	Oh is that dangerous?
Senecal:	**U can cum right**
Undercover:	Ummm yeah duh Lolol
Senecal:	**No not dangerous just give you a little bit to see how you react**
Undercover:	Yeah I'd be down
Senecal:	**Get into a lot so don't be afraid ok**
Undercover:	Ok I won't…What else would u want to do
Senecal:	**Water [image of three water droplets inserted]**
Undercover:	??
Senecal:	**Sweaty and raunchy Piss**
Undercover:	What do u mean?
Senecal:	**Piss in each other with chem piss**
Senecal:	**Up your ass**
Undercover:	Wow I've ever done that…u want to piss in my ass?
Senecal:	**Fuck both ways suck both ways make out lick chem sweat off each other**
Undercover:	I'd def do that…what's chem sweat?
Senecal:	**Yes you're doing the same to me**
Senecal:	**From the T**
Undercover:	Oh cool! Do u have a lot of T? Will we need a lot?
Senecal:	**I can get as soon as my funds come through**
Senecal:	**I do .5 to .8 I'll start you off with .1 for now can give you more once I see how you take it**
Senecal:	**U cool with that**
Senecal:	**Eat ass**
Undercover:	Ok cool yea I am as long as you take care of me
Undercover:	I don't want to get hurt
Senecal:	**I won't hurt you just party and sex**

16. On April 6, 2022, SENECAL and Detective Corporal Schatz continued their discussion of meeting at the Walmart on Post Road in Warwick. SENECAL advised he would be taking the public RIPTA bus to meet him. At 1:07 PM, SENECAL sent the following message, "On 1st bus". At 2:18 PM, SENECAL sent the following text message, "At airport waiting on bus 1".

17. At this time, detectives with the RISP ICAC Task Force, to include Detective Sergeant Marc Alboum, Detective Corporals Brian Macera and Adam Houston, Detectives Anthony

Washington, Brent Wilks, Ian Andrade, Patrick Smith (Warwick Police), HSI Special Agent James Richardson, Trooper Betsy Heidel, and Detective Corporal Schatz, initiated surveillance of the Walmart on Post Road in Warwick and of the bus stop at the T.F. Green airport arrival area on Post Road in Warwick. Corporal Macera and Detective Smith observed an individual who they identified as Richard SENECAL, YOB1960, waiting at the bus stop at the T.F. Green Airport arrival area. Corporal Macera and Detective Smith maintained constant surveillance of Richard Senecal as he entered the next RIPTA bus to arrive at the airport and traveled on that bus directly to the Walmart on Post Road in Warwick.

18. From a position of surveillance at the Walmart, Detective Corporal Schatz observed SENECAL exit the RIPTA bus and walk to the front of the Walmart store. SENECAL plugged his phone charger and phone into an outlet on the exterior of the Walmart and waited to the right of the main entrance. At this time, members of the surveillance team approached SENECAL and placed him into custody. The TARGET DEVICE was located plugged into an outlet between some vending machines at the Walmart. SENECAL identified the TARGET DEVICE as being his, and it was subsequently seized. Detective Corporal Schatz advised SENECAL of his *Miranda* rights on scene and SENECAL was transferred to the Wickford Barracks. At the barracks, Detective Corporal Schatz provided SENECAL a written copy of his *Miranda* rights. SENECAL signed the rights form and immediately requested an attorney and was not interrogated. SENECAL was processed and charged with three (3) counts of Indecent Solicitation of a Child and two (2) counts of Electronically Disseminating Indecent Material to a Minor. A Justice of the Peace responded to the Barracks and arraigned SENECAL. Bail was set at $10,000 with surety with a 3rd District Court date of April 7, 2022. SENECAL could not post bail and was

transported to the ACI Intake facility pending his arraignment in 3rd District Court the following day.

19. On April 7, 2022, SENECAL appeared for arraignment in 3rd District Court. Bail was set at $30,000 with surety with special bail conditions of no unsupervised contact with minors and restricted internet use. SENECAL was later presented in Superior Court as a bail violator. SENECAL is currently held without bail at the ACI.

SEARCH AND SEIZURE OF COMPUTER SYSTEMS AND DATA

20. Based on my knowledge, training, experience, and information provided to me by other agents, I know that computer files or remnants of such files can be recovered from cell phones months or even years after they have been written, downloaded, saved, deleted, or viewed locally or over the Internet. This is true because:

    a. Electronic files that have been downloaded to a storage medium can be stored for years at little or no cost. Furthermore, when users replace their computers, they can easily transfer the data from an old computer to a new computer.

    b. Even after files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data, which might not occur for long periods of time. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

    c. Wholly apart from user-generated files, computer storage media – in particular, computers' internal hard drives – contain electronic evidence of how the computer has been used, what it has been used for, and who has used it. This evidence can

take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. It is technically possible to delete this information, but computer users typically do not erase or delete this evidence because special software is usually required for that task.

d. Similarly, files that have been viewed over the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache." The browser often maintains a fixed amount of hard drive space devoted to these files, and the files are overwritten only as they are replaced with more recently viewed Internet pages or if a user takes steps to delete them.

21. Based on my knowledge and training and the experience of other agents with whom I have spoken, I am aware that in order to completely and accurately retrieve data maintained in computer hardware, computer software, or storage media, to ensure the accuracy and completeness of such data, and to prevent the loss of the data either from accidental or programmed destruction, it is often necessary that computer hardware, computer software, computer-related documentation, and storage media ("computer equipment") be seized and subsequently processed by a qualified computer specialist in a laboratory setting, rather than in the location where it is seized. This is true because of:

a. The volume of evidence: Storage media such as cellular phones can store the equivalent of thousands or, in some instances, millions of pages of information. Additionally, a user may seek to conceal evidence by storing it in random order or with deceptive file names. Searching authorities may need to examine all the stored data to determine what particular files are evidence, fruits, or instrumentalities of

criminal activity. This process can take weeks or months, depending on the volume of data stored, and it would be impractical to attempt this analysis on-site.

b. Technical requirements: Analyzing cellular phones and/or storage media for criminal evidence is a highly technical process requiring training and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications. Furthermore, data analysis protocols are exacting procedures, designed to protect the integrity of the evidence and to recover even "hidden," deleted, compressed, password-protected, or encrypted files. Many commercial computer software programs also save data in unique formats that are not conducive to standard data searches. Additionally, computer evidence is extremely vulnerable to tampering or destruction, both from external sources and destructive code imbedded in the system as a "booby trap."

CONCLUSION

22. Based on the foregoing, I submit that there is probable cause to believe that evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 1470 (transfer of obscene material to a minor) and 2422(b) (attempted enticement of a minor to engage in illicit sexual activity), as described in Attachment B, are located within the TARGET DEVICE, as more fully described in Attachment A.

Respectfully Submitted,

Michael Agostinho
Special Agent
Department of Homeland Security

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by:
telephone.
(specify reliable electronic means)

Date	Judge's signature
Providence, Rhode Island City and State	Lincoln D. Almond, US Magistrate Judge Printed name and title

ATTACHMENT A

DESCRIPTION OF PROPERTY TO BE SEARCHED

The TARGET DEVICE is in the custody of HSI Providence and is located at 1 International Way, Warwick, RI 02886. The TARGET DEVICE is:

1. A black MOTOROLA SCHOK cell phone.

ATTACHMENT B

DESCRIPTION OF INFORMATION TO BE SEIZED

I. All records, in whatever form, and tangible objects that constitute evidence, fruits, or instrumentalities of 18 U.S.C §§ 1470 and 2422(b), including:

A. Records and tangible objects pertaining to the following topics:

1. Child pornography, child erotica and obscenity or the sexual abuse or exploitation of children;

2. Transportation and travel records and other indicia of travel;

3. Any images, videos or other media depicting sexual activity, child pornography or otherwise documenting the communications between SENECAL and the Under Cover officer and any other minors with whom SENECAL may have been communicating;

4. Communications between SENECAL and the Under Cover officer and with any other person that relates to the sexual exploitation of children; and

5. The identity of any child depicted in videos and photographs located in the equipment or discussed in any communications related to the sexual abuse or exploitation of children;

6. Any communication(s) relating to child pornography, the sexual abuse or exploitation of children, or the identity of any child depicted in videos and photographs located in the equipment;

7. The identity of any person who sent or received communication(s) relating to child pornography, the sexual abuse or exploitation of children, or the identity of any child depicted in videos and photographs located in the equipment;

8. Any social media account(s) used to send or receive any communication(s) relating to child pornography, the sexual abuse or exploitation of children, MV,

or the identity of any child depicted in videos and photographs located in the equipment

9. The travel or whereabouts of SENECAL on October 5 through October 6, 2021 and April 4 through April 6, 2022;

10. Evidence of who used, owned, or controlled the equipment;

11. Evidence of the times the equipment was used;

12. The identity, location, and travel of any co-conspirators;

13. Passwords, encryption keys, and other access devices that may be necessary to access the equipment;

14. Evidence of the equipment's Internet activity, including IP addresses used to connect to the internet, firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

15. Evidence of the attachment of other hardware or storage media;

16. Evidence of counter forensic programs and associated data that are designed to eliminate data;

17. Contextual information necessary to understand the evidence described in Attachments A and B.

II. Serial numbers and any electronic identifiers that serve to identify the TARGET DEVICE.

DEFINITIONS

For the purpose of this warrant:

A. "Equipment" means any hardware, software, storage media, and data.

B. "Hardware" means any electronic device capable of data processing (such as a computer, digital camera, cellular telephone, iPhone and or smartphone, wireless communication device, or GPS navigation device); any peripheral input/output device (such as a keyboard, printer, scanner, monitor, and drive intended for removable storage media); any related communication device (such as a router,

wireless card, modem, cable, and any connections), and any security device, (such as electronic data security hardware and physical locks and keys).

C. "Software" means any program, program code, information or data stored in any form (such as an operating system, application, utility, communication and data security software; a log, history or backup file; an encryption code; a user name; or a password), whether stored deliberately, inadvertently, or automatically.

D. "Storage media" means any media capable of collecting, storing, retrieving, or transmitting data (such as a hard drive, CD, DVD, USB or thumb drive, or memory card).

E. "Data" means all information stored on storage media of any form in any storage format and for any purpose.

F. A "record" is any communication, representation, information or data. A "record" may be comprised of letters, numbers, pictures, sounds or symbols.